

Sub  
a7  
What is claimed is:

1. A computer program product for enabling a subsequent user sign-on during a certificate-based host access session, said computer program product embodied on a computer-readable medium and comprising:

computer-readable program code means for processing a first sign-on during a secure session using a digital certificate, further comprising:

computer-readable program code means for establishing said secure session from a client machine to a server machine using said digital certificate, wherein said digital certificate represents an identity of said client machine or a user thereof;

computer-readable program code means for storing said digital certificate or a reference thereto at said server machine;

computer-readable program code means for establishing a session from said server machine to a host system using a legacy host communication protocol;

computer-readable program code means for passing said stored digital certificate or said reference from said server machine to a host access security system;

computer-readable program code means, operable in said host access security system, for authenticating said identity using said passed digital certificate or a retrieved certificate which is retrieved using said reference;

computer-readable program code means for using said passed or retrieved digital certificate to locate access credentials for said user;

computer-readable program code means for accessing a stored password or generating a password substitute representing said located credentials; and

22 computer-readable program code means for using said stored password or said  
23 generated password substitute to transparently complete said first sign-on to a secure legacy host  
24 application executing at said host system; and

25 computer-readable program code means for processing a subsequent sign-on during said  
26 secure session using said digital certificate, wherein said subsequent sign-on requests access to  
27 said secure legacy host application or a different legacy host application, further comprising:

28 computer-readable program code means for receiving a subsequent sign-on  
29 request requiring said identity;

30 computer-readable program code means for retrieving said stored digital  
31 certificate or reference;

32 computer-readable program code means for passing said retrieved digital  
33 certificate or reference from said server machine to said host access security system;

34 computer-readable program code means, operable in said host access security  
35 system, for re-authenticating said identity using said passed retrieved digital certificate or  
36 retrieved reference;

37 computer-readable program code means, operable in said host access security  
38 system, for using said passed retrieved digital certificate or retrieved reference to again re-locate  
39 said access credentials for said user;

40 computer-readable program code means for re-accessing said stored password or  
41 generating a new password substitute representing said re-located credentials; and

42 computer-readable program code means for using said re-accessed stored  
43 password or said new password substitute to transparently complete said subsequent sign-on to

44 said secure legacy host application executing at said host system or said different legacy host  
45 application.

1 2. The computer program product as claimed in Claim 1, wherein said digital certificate is  
2 an X.509 certificate and said digital certificate reference is a reference to an X.509 certificate.

1 3. The computer program product as claimed in Claim 1, wherein said communication  
2 protocol is a 3270 emulation protocol.

4. The computer program product as claimed in Claim 1, wherein said communication  
protocol is a 5250 emulation protocol.

5. The computer program product as claimed in Claim 1, wherein said communication  
protocol is a Virtual Terminal protocol.

6. The computer program product as claimed in Claim 3, wherein said host access security  
system is a Resource Access Control Facility (RACF) system.

7. The computer program product as claimed in Claim 1, wherein said server machine is a  
Web application server machine.

8. The computer program product as claimed in Claim 1, further comprising:

2 computer-readable program code means for requesting by said legacy host application,  
3 responsive to said computer-readable program code means for establishing said session, first  
4 sign-on information for said user;

5 computer-readable program code means for responding to said request for first sign-on  
6 information by sending a first sign-on message with placeholders from said client machine to  
7 said server machine, said placeholders representing a user identification and a password of said  
8 user;

9 computer-readable program code means for substituting a user identifier associated with  
10 said located access credentials and said stored password or said generated password substitute for  
11 said placeholders in said first sign-on message;

12 computer-readable program code means for requesting, by said legacy host application,  
13 subsequent sign-on information for said user;

14 computer-readable program code means for responding to said request for subsequent  
15 sign-on information by sending a subsequent sign-on message with placeholders from said client  
16 machine to said server machine, said placeholders representing said user identification and said  
17 password of said user; and

18 computer-readable program code means for substituting said user identifier associated  
19 with said re-located access credentials and said re-accessed stored password or said new  
20 password substitute for said placeholders in said subsequent sign-on message.

1 9. The computer program product as claimed in Claim 7, further comprising:

2 computer-readable program code means for requesting by said legacy host application,

responsive to said computer-readable program code means for establishing said session, first sign-on information for said user;

computer-readable program code means for responding to said request for first sign-on information by supplying a user identifier associated with said located access credentials and said stored password or said generated password substitute at said server machine;

computer-readable program code means for requesting, by said legacy host application, subsequent sign-on information for said user; and

computer-readable program code means for responding to said request for subsequent sign-on information by supplying said user identifier associated with said re-located access credentials and said re-accessed stored password or said new password substitute at said server machine.

10. A system for enabling a subsequent user sign-on during a certificate-based host access session, comprising:

means for processing a first sign-on during a secure session using a digital certificate, further comprising:

means for establishing said secure session from a client machine to a server machine using said digital certificate, wherein said digital certificate represents an identity of said client machine or a user thereof;

means for storing said digital certificate or a reference thereto at said server machine;

means for establishing a session from said server machine to a host system using a

11 legacy host communication protocol;

12 means for passing said stored digital certificate or said reference from said server  
13 machine to a host access security system;

14 means, operable in said host access security system, for authenticating said  
15 identity using said passed digital certificate or a retrieved certificate which is retrieved using said  
16 reference;

17 means for using said passed or retrieved digital certificate to locate access  
18 credentials for said user;

19 means for accessing a stored password or generating a password substitute  
20 representing said located credentials; and

21 means for using said stored password or said generated password substitute to  
22 transparently complete said first sign-on to a secure legacy host application executing at said host  
23 system; and

24 means for processing a subsequent sign-on during said secure session using said digital  
25 certificate, wherein said subsequent sign-on requests access to said secure legacy host application  
26 or a different legacy host application, further comprising:

27 means for receiving a subsequent sign-on request requiring said identity;

28 means for retrieving said stored digital certificate or reference;

29 means for passing said retrieved digital certificate or reference from said server  
30 machine to said host access security system;

31 means, operable in said host access security system, for re-authenticating said  
32 identity using said passed retrieved digital certificate or retrieved reference;

33 means, operable in said host access security system, for using said passed  
34 retrieved digital certificate or retrieved reference to again re-locate said access credentials for  
35 said user;

36 means for re-accessing said stored password or generating a new password  
37 substitute representing said re-located credentials; and

38 means for using said re-accessed stored password or said new password substitute  
39 to transparently complete said subsequent sign-on to said secure legacy host application  
40 executing at said host system or said different legacy host application.

11. The system as claimed in Claim 10, wherein said digital certificate is an X.509 certificate  
and said digital certificate reference is a reference to an X.509 certificate.

12. The system as claimed in Claim 10, wherein said communication protocol is a 3270  
emulation protocol.

13. The system as claimed in Claim 12, wherein said host access security system is a  
Resource Access Control Facility (RACF) system.

14. The system as claimed in Claim 10, wherein said server machine is a Web application  
server machine.

15. The system as claimed in Claim 10, further comprising:

2 means for requesting by said legacy host application, responsive to said means for  
3 establishing said session, first sign-on information for said user;

4 means for responding to said request for first sign-on information by sending a first sign-  
5 on message with placeholders from said client machine to said server machine, said placeholders  
6 representing a user identification and a password of said user;

7 means for substituting a user identifier associated with said located access credentials and  
8 said stored password or said generated password substitute for said placeholders in said first  
9 sign-on message;

10 means for requesting, by said legacy host application, subsequent sign-on information for  
11 said user;

12 means for responding to said request for subsequent sign-on information by sending a  
13 subsequent sign-on message with placeholders from said client machine to said server machine,  
14 said placeholders representing said user identification and said password of said user; and

15 means for substituting said user identifier associated with said re-located access  
16 credentials and said re-accessed stored password or said new password substitute for said  
17 placeholders in said subsequent sign-on message.

1 16. The system as claimed in Claim 14, further comprising:

2 means for requesting by said legacy host application, responsive to said means for  
3 establishing said session, first sign-on information for said user;

4 means for responding to said request for first sign-on information by supplying a user  
5 identifier associated with said located access credentials and said stored password or said



6 generated password substitute at said server machine;

7 means for requesting, by said legacy host application, subsequent sign-on information for  
8 said user; and

9 means for responding to said request for subsequent sign-on information by supplying  
10 said user identifier associated with said re-located access credentials and said re-accessed stored  
11 password or said new password substitute at said server machine.

1 17. A method for enabling a subsequent user sign-on during a certificate-based host access  
2 session, comprising the steps of:

3 processing a first sign-on during a secure session using a digital certificate, further  
4 comprising the steps of:

5 establishing said secure session from a client machine to a server machine using  
6 said digital certificate, wherein said digital certificate represents an identity of said client  
7 machine or a user thereof;

8 storing said digital certificate or a reference thereto at said server machine;

9 establishing a session from said server machine to a host system using a legacy  
10 host communication protocol;

11 passing said stored digital certificate or said reference from said server machine to  
12 a host access security system;

13 authenticating, by said host access security system, said identity using said passed  
14 digital certificate or a retrieved certificate which is retrieved using said reference;

15 using said passed or retrieved digital certificate to locate access credentials for

16 said user;

17 accessing a stored password or generating a password substitute representing said  
18 located credentials; and

19 using said stored password or said generated password substitute to transparently  
20 complete said first sign-on to a secure legacy host application executing at said host system; and

21 processing a subsequent sign-on during said secure session using said digital certificate,  
22 wherein said subsequent sign-on requests access to said secure legacy host application or a  
23 different legacy host application, further comprising the steps of:

24 receiving a subsequent sign-on request requiring said identity;

25 retrieving said stored digital certificate or reference;

26 passing said retrieved digital certificate or reference from said server machine to  
27 said host access security system;

28 re-authenticating, by said host access security system, said identity using said  
29 passed retrieved digital certificate or retrieved reference;

30 using, by said host access security system, said passed retrieved digital certificate  
31 or retrieved reference to again re-locate said access credentials for said user;

32 re-accessing said stored password or generating a new password substitute  
33 representing said re-located credentials; and

34 using said re-accessed stored password or said new password substitute to  
35 transparently complete said subsequent sign-on to said secure legacy host application executing  
36 at said host system or said different legacy host application.

1 18. The method as claimed in Claim 17, wherein said digital certificate is an X.509 certificate  
2 and said digital certificate reference is a reference to an X.509 certificate.

1 19. The method as claimed in Claim 17, wherein said communication protocol is a 3270  
2 emulation protocol.

1 20. The method as claimed in Claim 19, wherein said host access security system is a  
2 Resource Access Control Facility (RACF) system.

1 21. The method as claimed in Claim 17, wherein said server machine is a Web application  
2 server machine.

1 22. The method as claimed in Claim 17, further comprising the steps of:  
2 requesting by said legacy host application, responsive to said step of establishing said  
3 session, first sign-on information for said user;  
4 responding to said request for first sign-on information by sending a first sign-on message  
5 with placeholders from said client machine to said server machine, said placeholders representing  
6 a user identification and a password of said user;  
7 substituting a user identifier associated with said located access credentials and said  
8 stored password or said generated password substitute for said placeholders in said first sign-on  
9 message;  
10 requesting, by said legacy host application, subsequent sign-on information for said user;

11 responding to said request for subsequent sign-on information by sending a subsequent  
12 sign-on message with placeholders from said client machine to said server machine, said  
13 placeholders representing said user identification and said password of said user; and  
14 substituting said user identifier associated with said re-located access credentials and said  
15 re-accessed stored password or said new password substitute for said placeholders in said  
16 subsequent sign-on message.

1 23. The method as claimed in Claim 21, further comprising the steps of:

2 requesting by said legacy host application, responsive to said step of establishing said  
3 session, first sign-on information for said user;

4 responding to said request for first sign-on information by supplying a user identifier  
5 associated with said located access credentials and said stored password or said generated  
6 password substitute at said server machine;

7 requesting, by said legacy host application, subsequent sign-on information for said user;  
8 and

9 responding to said request for subsequent sign-on information by supplying said user  
10 identifier associated with said re-located access credentials and said re-accessed stored password  
11 or said new password substitute at said server machine.